REMARKS/ARGUMENTS

In the Office Action, the Examiner noted that claims 1-9, 11-29, 31-35, and 37-57 are pending in the application. The Examiner additionally stated that claims 1-9, 11-29, 31-35, and 37-57 are rejected. By this amendment, claims 5 and 53 have been cancelled and claims 1, 6-9, 31, 40, and 54-57 have been amended. Hence, claims 1-4, 6-9, 11-29, 31-35, 37-52, and 54-57 are pending in the application.

Applicant hereby requests further examination and reconsideration of the application, in view of the foregoing amendments.

In the Specification

Applicant has amended the specification to secure a substantial correspondence between the claims amended herein and the remainder of the specification. No new matter is presented.

In the Claims

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 1-9, 11-29, 31-35, and 37-39 under 35 U.S.C. 103(a) as being unpatentable over Hashimoto et al., US 6,983,374 (hereinafter, "Hashimoto"), and further in view of Muratani et al., US 7,194,090 (hereinafter, "Muratani"). Applicant respectfully traverses the Examiner's rejections.

Regarding claim 1, the Examiner noted that Hashimoto discloses an apparatus for performing cryptographic operations, comprising:

- a cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, be executed on a plurality of input text blocks; and (col.10, lines 37-60 and co1.28, lines 34-42)
- execution logic, operatively coupled to said cryptographic instruction, configured to execute said one of the cryptographic operations, wherein said execution logic comprises (col. 5, lines 58-67 and col. 10, lines 5-8):

- a cryptography unit, configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit, and wherein said plurality of input text blocks are retrieved from memory, and wherein said plurality of output text blocks are stored to said memory; (col. 11, lines 60-65)

- wherein said one of the cryptographic operations comprises:
  - indicating whether said one of the cryptographic operations has been interrupted by an interrupting event. (col.6, lines 1-18 and col.12, lines 52- 55 and col.13, lines 16-20; The Examiner asserted that Hashimoto discloses the execution of the program is often interrupted by an exception (or interruption) processing of the processor caused by the input/output or the like (col.9, lines 38-40 and col.27, lines 29-31), and thus, Hashimoto reads on the claimed interrupting event).

The Examiner noted that Hashimoto discloses a cryptography unit but did not further include a plurality of cryptographic rounds. The Examiner further stated that Murantani discloses an encryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption (col. 3, lines 19-23), noting that Murantani discloses the round function as the claimed cryptographic rounds where the common key encryption system employing expanded keys in a reversed order between for encryption and for decryption (col. 7, lines 10-17). The Examiner further pointed out that Murantani discloses this leads to an advantage that a single device for encryption/decryption purpose can be small sized and that it is possible to generate an expanded key from a common key in an on-the-fly manner without consumption of the conventional unnecessary delay time or storage capacity (col. 9, lines 38-51 and col. 10, lines 20-32).

The Examiner therefore concluded that it would have been obvious for a person of ordinary skills in the art to combine the teaching of Hashimoto with Murantani teaching cryptographic rounds or round functions because this leads to an advantage that a single device for encryption/decryption purpose can be small sized and that it is possible to generate an expanded key from a common key in .an on-the-fly manner without consumption of the conventional unnecessary delay time or storage capacity (Murantani - col. 9, lines 38-51 and col. 10, lines 20-32).

As in the previous response, Applicant respectfully disagrees with the Examiner's characterization of Hashimoto and the rejection of claim 1. Applicant notes that Hashimoto's invention is directed toward the secure execution of an application program with has been encrypted in memory (Fig. 2, 2203) and for which an encrypted key (Fig. 2, 2205) is provided at a location keyaddr. Hashimoto teaches an encryption execution start instruction (execcenc keyaddr) which directs his processor to decrypt the encrypted key at keyaddr and which stores the key in a secret key register (Fig. 1, 2115). The contents of the secret key register 2115 are subsequently used to decrypt instructions of the encrypted application program which have been fetched from memory 2103 via a BIU 2118. The decrypted instructions are stored in an instruction buffer 2113 and are executed by an instruction execution unit 2112.

Hashimoto teaches provisions for the execution of an application program which has not been encrypted (i.e., "plaintext program"), and also for protecting the context information of an encrypted application program which is interrupted. (See, for example, col. 16, lines 23-40). Clearly, Hashimoto's invention is provided to protect an application program (and corresponding context information) from tampering.

But what Hashimoto does not teach, and which is provided for by the present invention, as recited in claim 1, is a cryptography unit, configured execute a plurality of cryptographic rounds on each of a plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit, and wherein said plurality of input text blocks are retrieved from

memory, and wherein said plurality of output text blocks are stored to said memory. In other words, the present invention offers a programmer the ability to provide input text blocks in memory and to direct a computing device, via a cryptographic instruction, to perform cryptographic rounds on the input text blocks to generate corresponding output text blocks, which are stored to memory.

Although Hashimoto's device does indeed retrieve instructions for execution from memory, his device clearly does not perform a prescribed cryptographic operation on the instructions, for there is no way for a programmer to prescribe the cryptographic operation. Hashimoto's device always decrypts instructions that are retrieved from memory, and furthermore executes those instructions. Accordingly, Hashimoto does not teach generating a corresponding plurality of output data blocks, nor does he teach or suggest storing the output data blocks to memory. In rejection of these limitations of claim 1, the Examiner referred Applicant to Hashimoto col. 11, lines 60-65. Applicant provides this citation below:

> which takes no operand. By execution of this instruction, the reading of the instructions from the main memory **2103** is carried out through a path that does not pass through the common key decryption function **2116**, and the processor returns to the execution of the plaintext instructions.

It is unquestionable that Hashimoto fails to teach the generation of a corresponding plurality of output data blocks and storing these output data blocks to memory. Hashimoto is not motivated to provide for such a limitation because Hashimoto's technique does not contemplate a need to generate a corresponding plurality of output data blocks because Hashimoto's device is limited to execution of an encrypted set of program instructions, so called trusted computing.

Hashimoto's teachings are limited to the execution of encrypted application programs and do not address general purpose cryptography, as is taught in the instant application. In fact, according to the present invention, any type of data may be stored in memory as input text blocks (e.g., data or program instructions), and the computing device be

directed via the cryptographic instruction to either encrypt or decrypt the input text blocks. The corresponding output text blocks are then stored to memory.

Furthermore, Hashimoto utterly fails to teach or suggest a cryptographic instruction that prescribes one of the cryptographic operations. Hashimoto teaches two instructions: an encryption execution start instruction (col. 10, lines 47-54) and a plaintext return instruction (col. 11, line 53 through col. 12, line 3), neither of which prescribe one of a plurality of cryptographic operations.

Moreover, amended claim 1 recites that the cryptographic instruction also prescribes one of a plurality of block cipher modes to be employed in accomplishing said one of the cryptographic operations. Hashimoto is utterly silent in this respect. In rejection of claim 5, herein cancelled, the Examiner noted that Hashimoto on col. 11, lines 13-16; discussed the apparatus as recited in claim 1., wherein said cryptographic instruction prescribes a block cipher mode to be employed in accomplishing said one of the cryptographic operations. For ease of reference, the noted section of Hashimoto is provided below.

> In the following, the encryption execution start instruction and the subsequent the execution of the encrypted instruction will be described in detail. By the execution of the Jump instruction in a region **2207**, the control is shifted to the

Applicant respectfully notes that the provided section says nothing about a block cipher mode. And the only reference to a block cipher mode in Hashimoto is found in col. 18, lines 13-18, where he discusses how to create a mutual dependence between data blocks when encrypting program code But regarding the limitation of claim 1, Hashimoto is silent.

Applicant asserts that at the highest level of abstraction, the teaching of Hashimoto is quite distinct from that subject matter recited by claim 1 because Hashimoto does not address a programmable instruction that can be embedded in a program flow directing a device to retrieve input data blocks from memory, to employ a specified block cipher mode when processing (i.e., performing a prescribed cryptographic operation) the input data blocks, to generate a corresponding plurality of output data blocks, and to store these

output data blocks to memory. Hashimoto does not even consider such a function, for all he is concerned with is decrypting secure program code and executing the code.

Applicant does not dispute that Murantani discloses an encryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption. Applicant also does not disagree that Murantani discloses a round function, for performing cryptographic rounds is consistent with many prevalent cryptographic algorithms such as AES and DES. And in addition, Applicant notes that Murantani's statement that using the same hardware for key expansion as is used for decryption/encryption only follows from the fact that, for many cryptographic algorithms, these two functions employ the same operations (e.g., S-box, inverse). Consequently, all that Muratani teaches is that cryptography involves cryptographic rounds and that it is advantageous to use the same hardware to perform the same function. Muratani clearly does not teach or suggest any of the significant features of the instant invention recited in claim 1, to include a cryptographic instruction that specifies a block cipher mode.

Accordingly, it is requested that the rejection of claim 1 be withdrawn.

With respect to claims 2-4, 6-9, and 11-29, these claims depend from claim 1 and add further limitations that are neither anticipated nor made obvious by Hashimoto, Muratani, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 2-4, 6-9, and 11-29.

By this amendment, claim 5 is cancelled, thereby rendering the Examiner's rejection moot.

As per claim 31, the Examiner stated that Hashimoto teaches the apparatus for performing cryptographic operations, comprising:

- a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic

operations; and (col. 10, lines 37-60 and col. 28, lines 34-42) and wherein said cryptography unit is configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output data blocks, and wherein said plurality of input data blocks are retrieved from memory, and wherein said plurality of output data blocks are retrieved from memory; and (col. 11, lines 60-65);

- block pointer logic, operatively coupled to said cryptography unit, configured to direct said devices to modify pointers to said plurality of input and output data blocks in memory to point to next input and output data blocks at the completion of said one of the cryptographic operations on a current input data block; and (col. 11, lines 12-28 and col. 13, lines 42-47)

- a bit within a register (col. 26, lines 58-60 and col. 27, lines 59-62), operatively coupled to said cryptography unit, configured to indicate that execution of said one of the cryptographic operations has been interrupted an interrupting event. (col. 6, lines 1-18 and col. 12, lines 52-55 and col. 13, lines 16-20; noting that Hashimoto discloses the execution of the program is often interrupted by an exception (or interruption) processing of the processor caused by the input/output or the like (col. 9, lines 38-40 and col. 27, lines a 29-31), and thus, Hashimoto reads on the claimed interrupting event).

The Examiner noted that Hashimoto discloses a cryptography unit but did not further include a plurality of cryptographic rounds. The Examiner further stated that Murantani discloses an encryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption and in a reversed order in a data randomizing process for decryption (col. 3, lines 19-23), noting that Murantani discloses the round function as the claimed cryptographic rounds where the common key encryption system employing expanded keys in a reversed order between for encryption and for decryption (col. 7, lines 10-17). The Examiner further pointed out that Murantani discloses this leads to an advantage that a single device for encryption/decryption purpose can be small sized and

that it is possible to generate an expanded key from a common key in an on-the-fly manner without consumption of the conventional unnecessary delay time or storage capacity (col. 9, lines 38-51 and col. 10, lines 20-32).

The Examiner therefore concluded that it would have been obvious for a person of ordinary skills in the art to combine the teaching of Hashimoto with Murantani teaching cryptographic rounds or round functions because this leads to an advantage that a single device for encryption/decryption purpose can be small sized and that it is possible to generate an expanded key from a common key in .an on-the-fly manner without consumption of the conventional unnecessary delay time or storage capacity (Murantani - col. 9, lines 38-51 and col. 10, lines 20-32).

In reply, Applicant responds again that, like claim 1, claim 31 recites a cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, and wherein said cryptography unit is configured execute a plurality of cryptographic rounds on each of a plurality of input data blocks to generate a corresponding each of a plurality of output data blocks, and wherein said plurality of input data blocks are retrieved from memory, and wherein said plurality of output data blocks are stored to said memory. And as asserted above, Applicant points out that Hashimoto does not teach a cryptographic instruction that directs a device to retrieve input data blocks from memory, to perform a plurality of cryptographic rounds on the retrieved input data blocks to generate a corresponding output data blocks, and to store the output data blocks to memory. This is because Hashimoto's invention is solely directed toward the tamper-proof execution of an encrypted application program and not toward the above noted aspects of the present invention.

Hashimoto's teaching is silent with regard to specification of a cryptographic operation by way of a programmable instruction, and on specification of one of a plurality of block cipher modes to be employed. The citation sections noted by the Examiner as being relevant, as shown above, do not teach these limitations. Also, as argued above,

Hashimoto does not provide for generation of a corresponding plurality of output data blocks, or for storing these output data blocks to memory.

To support execution of cryptographic operations on the plurality of input text blocks in the presence of interrupting events, claim 31 also recites block pointer logic, operatively coupled to said cryptography unit, configured to direct said device to modify pointers to said plurality of input and output data blocks in memory to point to next input and output data blocks at the completion of said one of the cryptographic operations on a current input data block. The Examiner's note that col. 11, lines 12-28 disclose block pointer logic as recited is provided below:

> In the following, the encryption execution start instruction and the subsequent the execution of the encrypted instruction will be described in detail. By the execution of the Jump instruction in a region **2207**, the control is shifted to the encryption execution start instruction at the address "start". At the address indicated by the operand "keyaddr" of the encryption execution start instruction, the content of the specified region **2205** is read out to the instruction execution unit **2112** of the processor as data. The instruction execution unit **2112** sends this data $E_{Kp}[Kx]$ to the public key decryption function **2114**. The public key decryption function **2114** takes out Kx by decrypting $E_{Kp}[Kx]$ by using a secret key Ks unique to the processor which is stored in the secret key register **2115**, and stores it in the common key register **2117**. Then, the processor enters the encrypted instruction execution state.

As shown above, there is no reference to any element that is even analogous to block pointer logic as has been disclosed in the instant application. Thus, Hashimoto does not teach or suggest such an element or it's limitations. He has no need to do so, for his invention is solely concerned with decrypting secure program code for execution, not for performing a prescribed one of a plurality of cryptographic operations and block cipher modes on input data blocks to generate corresponding output data blocks, and to store these output data blocks to memory.

Furthermore, as argued above, all that Muratani brings of relevance is that cryptography involves cryptographic rounds and that it is advantageous to use the same hardware to

perform the same function. Muratani clearly does not teach or suggest any of the significant features of the instant invention recited in claim 31, to include a cryptographic instruction that specifies a block cipher mode.

Accordingly, it is requested that the rejection of claim 31 be withdrawn.

With respect to claims 32-35, and 37-39, these claims depend from claim 31 and add further limitations that are neither anticipated nor made obvious by Hashimoto, Muratani, or a combination of the two references. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 32-35 and 37-39.

Rejections Under 35 U.S.C. §103(a)

The Examiner rejected claims 40-57 under 35 U.S.C. 102(b) as being anticipated by Hashimoto. Applicant respectfully traverses the rejections.

With respect to claim 40, the Examiner opined that Hashimoto discloses a method for performing cryptographic operations in a device, the method comprising:

- retrieving a plurality of input data blocks from memory; (col. 11, lines 60-65);
- executing one of the cryptographic operations on the plurality of input of data blocks to generate a corresponding plurality of output data blocks (col. 5, lines 58-67), wherein said executing is performed responsive to receiving a cryptographic instruction, and wherein the cryptographic instruction prescribes the one of the cryptographic operations; (col. 10, lines 37-60 and col. 28, lines 34-42)
- storing the corresponding plurality of output data blocks to the memory; and (col. 11, lines 24-26) indicating whether an interrupting event has occurred during said executing. (col. 6, lines 1-18 and col. 12, lines 52-55 and col. 13, lines 16-20; noting that Hashimoto discloses the execution of the program is often interrupted by an exception (or interruption) processing of the processor caused by the input/output or the like (col. 9, lines 38-40 and col. 27, lines 29-31). Thus, the Examiner concluded that Hashimoto reads on the claimed interrupting event.)

Applicant respectfully disagrees again and notes that amended claim 40 recites, among other elements and limitations:

- fetching a cryptographic instruction from memory, wherein the cryptographic instruction prescribes one of the cryptographic operations along with one of a plurality of block cipher modes to be employed when performing the one or the cryptographic operations;
- employing the one of a plurality of block cipher modes and executing the one of the cryptographic operations on the plurality of input data blocks to generate a corresponding plurality of output data blocks, wherein said executing is performed responsive to said fetching, ;
- storing the corresponding plurality of output data blocks to the memory.

As has been highlighted above in the traversals of the rejections of claims 1 and 31, Applicant respectfully points out that Hashimoto does not teach or otherwise disclose an instruction for use by a devices that specifies both one of a plurality of cryptographic operations and one of a plurality of block cipher modes, that directs the device to retrieve input data blocks from memory and to perform the specified cryptographic operation thereon using the block cipher mode to generate corresponding output data blocks, which are then stored to memory.

Accordingly, it is requested that the rejection of claim 40 be withdrawn.

With respect to claims 41-52 and 54-57, these claims depend from claim 40 and add further limitations that are neither anticipated nor made obvious by Hashimoto. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejections of claims 41-52 and 54-57.

By this amendment, claim 53 is cancelled, rendering the rejection moot

RECEIVED
CENTRAL FAX CENTER
OCT 22 2007

CONCLUSIONS

Applicant believes this to be a complete response to all of the issues raised in the instant office action and further submits, in view of the amendments and arguments advanced above, that claims 1-4, 6-9, 11-29, 31-35, and 37-52, and 54-57 are in condition for allowance. Reconsideration of the rejections is requested, and allowance of the claims is solicited.

Applicant also notes that any amendments made by way of this response, and the observations contained herein, are made solely for the purpose of expediting the patent application process in a manner consistent with the PTO's Patent business Goals (PBG), 65 Fed. Reg. 54603 (September 8, 2000), and are furthermore made without prejudice to Applicant under this or any other jurisdictions. It is moreover asserted that insofar as any subject matter might otherwise be regarded as having been abandoned or effectively disclaimed by virtue of amendments made herein and/or incorporated in attachments submitted with this response, Applicants wishes to reserve the right and hereby provides notice of intent to restore such subject matter and/or file a continuation application in respect thereof.

Applicant earnestly requests that the Examiner contact the undersigned practitioner by telephone if the Examiner has any questions or suggestions concerning this amendment, the application, or allowance of any claims thereof.

I hereby certify under 37 CFR 1.8 that this correspondence is being facsimile transmitted to the United States Patent and Trademark Office on the date of signature shown below.

Respectfully submitted,
HUFFMAN PATENT GROUP, LLC

/Richard K. Huffman/

By: _____

RICHARD K. HUFFMAN, P.E.
Registration No. 41,082
Tel: (719) 575-9998

10/21/2001

Date: _____